

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-196083

(43)Date of publication of application : 21.07.1999

---

(51)Int.Cl.

H04L 9/08

H04L 9/32

---

(21)Application number : 10-293845 (71)Applicant : THOMSON MULTIMEDIA SA

(22)Date of filing : 15.10.1998 (72)Inventor : CAMPINOS ARNALDO  
FISCHER JEAN-BERNARD

---

(30)Priority

Priority number : 97 9713022 Priority date : 17.10.1997 Priority country : FR

---

## (54) METHOD FOR TRANSFERRING SCRAMBLE KEY

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain the method for transferring a scramble key from a security element to a decoder.

SOLUTION: This transfer method is conducted in an input stage, a challenge stage and an opening stage. In the input stage, a security element, including a scramble key whose cipher, is decoded exchanges a message with a decoder, and as a result, the decoder has items consisting of data representing all or a part of the scramble key whose cipher is decoded and data representing data, capable of authenticating a smart card in a one-to-one form at the end of the input stage. In the challenge state, the data are transferred from the decoder to the smart card. As a result, which of the received data is disclosed is represented. Preferably, explicitness of the received data is conducted at random. In the opening stage, the smart card transfers data of all or a part of the scramble key the cipher of which is decoded to the decoder, together with the data capable of authenticating the smart card.

---

## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

---

## CLAIMS

---

[Claim(s)]

[Claim 1] In the approach of transmitting the scramble key decrypted from the security element (1) to the decoder (2) Data of the n beginnings outputted from the security element (1) (X1, Y) () (X2, Y), ..., (Xn, Y) are put in into a decoder (2) (M1, M2, and ...) It is Mj, ..., Mn phase and said n is two or more integers. The phase where each data into which it was put by said n beginnings consists of the first data (Xj) which make all or part (Y), and security element (1) of a scramble key (KD) which were decrypted attest, The 2nd n data (Z1, Y) ((Z2, Y), ... (it Zj(s))) (Zn, Y) to Y), ..., p data (Za1, Y) () (Za2, Y), ..., the data (d) that make it possible to choose (Zap, Y) are the phases of the challenge (C) transmitted to a security element (1) from a decoder (2). Said p is an integer smaller than n. Said each 2nd n data The phase which consists of the 2nd data (Xj) to which authentication of all of the decrypted scramble keys or a part (Y), and a security element (1) is carried out, The phase of opening (O1, O2, ..., Op) which consists of p data transfers chosen from the security element (1) as the decoder (2) in the challenge phase (C), the data (X1, Y) ((X2, Y), and ...) put into the n beginnings p data (O1 (Za1, Y) --) transmitted in p data and the opening phase which were chosen from (Xn, Y) The approach characterized by consisting of a count phase which makes it possible to extract all or the part (Y) of a scramble key decrypted from O2 (Za2, Y), ..., Op (Zap, Y).

[Claim 2] The approach according to claim 1 of consisting of a phase which reconstructs a perfect scramble key when said phase to put in, an opening phase, and a count phase relate to a part of perfect scramble key (KD) (Y) behind said count

phase.

[Claim 3] Said phase (M1, M2, ..., M<sub>j</sub>, ..., M<sub>n</sub>) to put in is the approach according to claim 1 or 2 consist of three steps (M1, M2, M3), and an opening step (O1, O2, ..., O<sub>p</sub>) consists of two steps.

[Claim 4] It is [ claim 1 performed at random thru/or ] an approach given in any 1 term among 3 to choose p data (Z<sub>a1</sub>, Y) ((Z<sub>a2</sub>, Y), ..., (Z<sub>ap</sub>, Y)) from the 2nd n data (Z<sub>1</sub>, Y) ((Z<sub>2</sub>, Y), ..., (Z<sub>j</sub>, Y), ..., (Z<sub>n</sub>, Y)).

[Claim 5] The data into which it was put by the n beginnings respectively (C<sub>j</sub>) It is as a result of the first exclusive-OR function (5) in which the first data (B<sub>j</sub>) and 2nd data (G<sub>j</sub>) are applied. Said first data (B<sub>j</sub>) It is the pseudo-random WORD generated with the application of seed (S<sub>j</sub>) in the first pseudo-random generation vessel (4). Said 2nd data (G<sub>j</sub>) It is the WORD generated from relating all or the parts of the 3rd data and the decrypted scramble keys (Y). Said opening phase consists of transmitting seed (S<sub>j</sub>) and the 2nd data (G<sub>j</sub>) to a decoder (2) from a security element (1). Said count phase In order to calculate the 4th data (E<sub>j</sub>) based on applying Seed S<sub>j</sub> to the 2nd pseudo-random generation machine (8) and to calculate the 5th data (F<sub>j</sub>) The 4th data (E<sub>j</sub>) and data (C<sub>j</sub>) into which it was put are applied to the 2nd exclusive-OR function (9). If the 5th data (F<sub>j</sub>) is the same as the 2nd data (G<sub>j</sub>) transmitted by opening operation as compared with the 2nd data (G<sub>j</sub>) to which the 5th data (F<sub>j</sub>) is transmitted by opening operation as a result of a comparison It is [ claim 1 which consists of storing decrypted all or the part (Y) of scramble keys thru/or ] an approach given in any 1 term among 4.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] the approach this invention transmits a scramble key -- being related -- especially -- conditional -- it is related with the approach of transmitting a scramble key between the security element of an access system, and a decoder. conditional -- only the user who acquired the access which receives the service for its service can be provided with a service provider by the access system. There are for example, charged television systems in such a system.

[0002]

[Description of the Prior Art] The service offered by the service provider consists of an item to which the scramble was able to be applied by the scramble key so that it may be well-known to this contractor. The item to which the scramble was able to be applied is the level of the access assigned to the user, has a scramble canceled and

is read by the user. The following [ the scrambled item ] IE (ECG) is written. ECG expresses the item which is not scrambled (ECG is the abbreviation for "Electronically Coded Goods").

[0003] In order to carry out scramble discharge of the item, a service provider supplies the scramble key used in order to scramble an item to each user. In order to maintain a scramble key at secrecy, a scramble key is supplied after being enciphered with the algorithm which used Key K. The scramble key as which versatility was enciphered is sent to various users in a control message. Hereafter, ECM [ a control message ] is written (ECM is the abbreviation for "Entitlement Control Message").

[0004] In order to give access to service only to the user who was able to grant access, a service provider provides each user with a smart card and a decoder. ECM is received by the decoder and a decoder transmits them to a smart card. A smart card contains the key K of the encryption algorithm of a scramble key. A scramble key is decoded by the smart card, it is restored by the decoder, and a decoder can carry out scramble discharge of the received item which was scrambled.

[0005]

[Problem(s) to be Solved by the Invention] The hacker who does the monitor of between a smart card and decoders is in the location which monitors the decrypted scramble key which flows from a smart card to a decoder. This expresses a fault. conditional -- an access system is a stand-alone type system, and since the items IE (ECG) and ECM scrambled in that system are included on the information carrier of a stand-alone like a digital videodisc, this fault is still more serious. It is because the hacker who monitors the scramble key which is not enciphered can store these keys and they of the user who has not obtained authorization can be redistributed unjustly. The scrambled item which is included on a stand-alone information carrier will already be protected.

[0006] conditional -- when an access system is an online type, the scrambled item IE (ECG) is an item which consists of signals to which the space or cable top was simultaneously distributed from the single source to the various customers of a service provider. The hack (disturbance) of the decoded scramble key must be carried out on real time. The conditions of hacking become more difficult. However, there is danger of hacking on a link short enough comparatively until now [ high ].

[0007] This invention does not have these faults.

[0008]

[Means for Solving the Problem] This invention relates to the approach of transmitting the scramble key decrypted from the security element to the decoder. The above-mentioned approach of carrying out a transfer consists of the next phase. - In a decoder, it is the phase of putting in n data output of the beginning from a security element (pledge), and, as for n, each n data of two or more integers and the beginning into which it was put consists of the first data to which authentication of all of the decrypted scramble keys or a part, and a security element is carried out.

[0009] – One data which makes it possible to choose p data from the 2nd n data is the phase of the challenge transmitted to a security element from a decoder, p is an integer smaller than n and each 2nd n data consists of all of the decrypted scramble keys or parts, and the 2nd data to which authentication of a security element is carried out.

[0010] – The phase of opening which consists of transmitting p data chosen between challenge phases to a decoder from a security element.

– The phase of the count which makes it possible to extract all or the part of scramble keys decrypted from p data chosen from the first n data into which it was put, and p data transmitted in the opening phase.

[0011] According to the specific embodiment of this invention, the method of transmitting the decrypted scramble key is as follows.

– Each first n data into which it was put is as a result of the first exclusive-OR function applied to the first data and 2nd data, the first data are pseudo-random WORD generated from adding seed to the first pseudo-random generation machine, and the 2nd data is WORD generated from being connected with all of the 3rd data and the decrypted scramble keys, or a part.

[0012] – An opening phase consists of transmitting seed and the 2nd data to a decoder from a security element.

– The phase of count consists of a degree.

– Calculate the 4th data based on applying seed to the 2nd pseudo-random generation machine.

[0013] – In order to calculate the 5th data, apply the 4th data and guaranteed data to the 2nd exclusive-OR function.

– Compare the 5th data with the 2nd data transmitted between actuation of opening.

– If it turns out that it is the same as that of the 2nd data with which the 5th data was transmitted between actuation of opening as a result of a comparison, store decrypted all or the part of scramble keys.

[0014] The advantage of this invention is protecting an exchange of the data between a security element and a decoder.

[0015]

[Embodiment of the Invention] Other descriptions and advantages of this invention become clear by reading one desirable embodiment of this invention with reference to an accompanying drawing. In the accompanying drawing, the same sign shows the same element. Drawing 1 shows fundamental drawing of the approach of transmitting the scramble key decrypted between the security element 1 and the decoder 2. A security element is a smart card preferably.

[0016] As mentioned above, a scramble key is transmitted to a decoder 2 from a smart card 1 according to the principle of operation of putting in (pledge). The principle of operation which puts in data consists of putting into the 2nd side about a beginning side, without transmitting without encryption about the data defined

beforehand. Next, a beginning side shows the data which are not enciphered to the 2nd side between the continuing steps. It has possibility of checking the data of the side [ 2nd ] which is not enciphered corresponding with the data into which it was put. [0017] According to this invention, a beginning side is a smart card 1, the 2nd side is a decoder 2 and the data into which it is put consist of decrypted all or the part of scramble keys. The protocol for exchanging data between a smart card and a decoder consists of three phases intrinsically [ the phase to put in (pledging), a challenge phase, and an opening phase ].

[0018] In the phase to put in, the smart card 1 containing the decrypted scramble key exchanges a decoder 2 and a message. In the end of the phase to put in, a smart card 1 exchanges a decoder 2 and a message by the approach of having the item which consists of data which enable a decoder to attest the data showing all or the part of scramble keys which is the form of 1 to 1 and was decrypted, and a smart card. Vocabulary called the data which make it possible to attest a smart card should be understood to be what means the data which make it possible to check that the hack (disturbance) of the smart card is not carried out.

[0019] The information included in the decoder in the end of a guarantee phase as an advantageous point cannot obtain the data for attesting all of the decrypted scramble keys or a part, and a card in itself. In a challenge phase, in order to show which should be indicated among the data into which it was put, data are transmitted to a smart card from a decoder. It performs by the approach with random the data which should be indicated and into which it was put being shown preferably.

[0020] In an opening phase, a smart card transmits the data which should be indicated by the decoder. That is, the data for attesting all of the decrypted scramble keys or a part, and a smart card are transmitted. A smart card 1 consists of the set  $(X_1, Y)$  of data,  $(X_2, Y), \dots, (X_n, Y)$ .

[0021] Each data  $(X_j, Y)$  ( $j = 1, 2, \dots, n$ ) consists of data  $Y$  and data  $X_j$ . Data  $Y$  are decrypted all or the part of a scramble key. Data  $X_j$  are independent of a scramble key, and are data which make a smart card attest. Arrow heads  $M_1, M_2, \dots, M_j, \dots, M_n, C, O_1, O_2, \dots, O_n$  show the various exchanges between a smart card 1 and a decoder 2.

[0022] It is shown that arrow heads  $M_1$  and  $M_2, \dots, M_j, \dots, M_n$  put in each data  $(X_1, Y), (X_2, Y), \dots, (X_n, Y)$ . Preferably, putting in  $M_{j+1}$  of data  $(X_{j+1}, Y)$  is performed after putting in  $M_j$  of data  $(X_j, Y)$ . According to the desirable embodiment of this invention, the phase to put in consists of three steps of  $M_1, M_2$ , and  $M_3$ . More generally the phase to put in consists of an  $n$  step, and  $n$  is two or more integers.

[0023] The data  $(X_j, Y)$  into which it was put by the decoder 2 are expressed as  $M_j (X_j, Y)$ . As an advantageous point, Data  $M_j (X_j, Y)$  cannot identify Data  $X_j$  and  $Y$  by itself as mentioned above. The arrow head  $C$  shows the challenge phase. In a challenge phase, the data  $d$  chosen at random preferably are transmitted to a smart card 1 from a decoder 2. According to an operation of Data  $d$ , the microprocessor of a smart card

1 transmits P data which chose p data and were chosen from n data (Z1, Y) contained in a smart card, (Z2, Y), ..., (Zj, Y), ..., (Zn, Y) in this way to a decoder 2 from a smart card 1.

[0024] Each data (Zj, Y) (j= 1, 2, ..., n) consists of data Y and data Zj. According to the embodiment of the beginning of this invention, Data Zj (j= 1, 2, ..., n) are the same as Data Xj, and the data (Zj, Y) of them are the same as data (Xj, Y).

[0025] According to other embodiments of this invention, Data Zj differ from Data Xj. According to the embodiment besides \*\*\*\*\* of this invention, Data Zj are carrying out mutual relation with Data Xj. An expression called the mutual relation of Data Zj and Data Xj is applied to data (Zj, Y) and (Xj, Y) various circuits, and/or an operator, and makes the extract of Data Y, and coincidence attest a smart card. The example of such an embodiment is explained by drawing 2.

[0026] n data (Z1, Y), (Z2, Y), ..., (Zj, Y), ..., p data chosen from (Zn, Y) consist of the set (Za1, Y) of data, (Za2, Y), ..., (Zap(s), Y). In the transfer to a decoder 2 from the smart card 1 of p data (Za1, Y), (Za2, Y), ..., (Zap, Y), arrow heads O1, O2, ..., Op express the opening of each data (Za1, Y), (Za2, Y), ..., (Zap, Y) in opening operation.

[0027] Each data (Za1, Y), (Za2, Y), ..., the data stored after the opening of (Zap, Y) at the decoder 2 are expressed as O1 (Za1, Y), O2 (Za2, Y), ..., Op (Zap, Y). Each p data Ok (Zak, Y) is in agreement with one of the data Mj (Xj, Y) into which it was put. An expression called the data Mj (Xj, Y) into which it was put, and the data Ok (Zak, Y) in agreement The data Ok (Zak, Y) whose data Zak correspond with Data Xj in the case of the embodiment of the beginning of this invention mentioned above, Or it should be understood that Data Zak mean Data Xj and the data Ok (Zak, Y) which are carrying out mutual relation in the case of other embodiments of this invention.

[0028] According to this invention, a decoder 2 extracts Data Y from the data Ok (Zak, Y) equivalent to Data Mj (Xj, Y) and Mj (Xj, Y), and consists of a means M0 which makes possible what a smart card 1 is attested for. Data Y are stored in memory circuit M when Data Y are extracted from Data Mj (Xj, Y) and Ok (Zak, Y) by the means M0.

[0029] According to the desirable embodiment of this invention, in an opening phase, the phase to put in relates to two data of (Za1, Y), and (Za2, Y) in relation to three data of (X1, Y), (X2, Y), and (X3, Y). Data Y are decrypted all or the part of scramble keys as mentioned above. When it is the part of the scramble key by which Data Y were decrypted, operation mentioned above is performed in each various parts which constitute a scramble key. If an example is given, each data Y which is the part of the decrypted scramble key will consist of 7 or 8 bits, and a scramble key will be thoroughly reconfigured with ten pass. Each pass makes a circuit M0 extract Data Y. Perfect reconstruction of the enciphered scramble key KD is performed using memory circuit M.

[0030] According to this invention, as an advantageous point, the transfer to a decoder 2 from the smart card 1 of Data Y is performed to authentication and

coincidence of a smart card 1. Since the data which the smart card was not attested any longer, consequently were transmitted to the decoder must have been taken into consideration, it becomes impossible so, for the hacker who monitors the data exchanged between a smart card and a decoder to find out semantics to change these data.

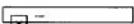
[0031] Drawing 2 expresses the specific embodiment of fundamental drawing shown in drawing 1 . Only putting in (pledging) and the operation of opening are expressed in drawing 2 . The various arrow heads from a smart card 1 to a decoder 2 express various exchanges of the data between a smart card 1 and a decoder 2.

[0032] The arrow head Mj means putting the data Cj contained in a smart card 1 into a decoder 2. Arrow heads Oa and Ob express the opening step equivalent to step Mj to put in. Since it is convenient, the exchange of the data between the smart cards 1 and decoders 2 which were expressed to drawing 2 relates to single step and single opening step. As mentioned above, according to the desirable embodiment of this invention, three data are put in by the decoder 2 and two opening steps (Oa, Ob) are actually performed from a smart card 1 to a decoder 2.

[0033] According to the specific embodiment of drawing 2 , a smart card 1 consists of the generation machine 3 of random WORD, the pseudo-random generation machine 4, an exclusive-OR function 5 6, for example, a data association circuit like a data connection circuit, and a separation operator 7, and a decoder 2 stores the pseudo-random generation machine 8, the exclusive-OR function 9, a comparison circuit 10, and the various data Y, and if required, it will consist of a circuit M which reconfigures the perfect key KD from the various data Y.

[0034] The false data generation machine 8, the exclusive-OR function 9, and a comparison circuit 10 constitute the example of a circuit M0. The data Cj into which it was put are generated by applying Data Bj and Data Gj to the exclusive-OR function 5. So, [0035]

[Equation 1]

 -

[0036] It can describe. Data Bj are pseudo-random WORD generated from the generation machine 4 with which Seed Sj is applied, and generate the seed Sj itself from the generation machine 3 of random WORD. Data Gj consist of WORD generated from association of Data Dj and Data Y. Association of Data Dj and Data Y is performed by connection.

[0037] According to the desirable embodiment of this invention, Data Y are the part of the decrypted scramble key KD which consists of b bits. As an example, b is equal to 7 or 8 bits respectively to the enciphered scramble key which consists of 70 or 80 bits. Data Y are generated from the separation circuit 7 where the decrypted scramble key KD is applied. The scramble key enciphered so that it might be well-known is transmitted to this contractor from a decoder 2 to a smart card 1, and a

smart card 1 includes the decryption circuit (it has not indicated to drawing 2 ) which makes it possible to restore the decrypted key KD.

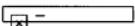
[0038] According to other embodiments of this invention, Data Y are the scramble key by which the whole was decrypted. According to this invention, an authentication procedure is activated whenever the enciphered scramble key is transmitted to a smart card 1 from a decoder 2. Since it is impossible to determine the data Bj generated from the pseudo-random generation machine 4, the expression with which 1 to 1 of the data Gj maintained at secrecy by Naka of Cj was enciphered is Data Cj.

[0039] If WORD Cj is transmitted to a decoder 2 from a smart card 1, the phase which Cj puts in will be completed. And an opening step is performed. In an opening step, two data Sj and Gj are transmitted to a decoder 2 from a smart card 1. Data Sj are transmitted by Opening Oa and Data Gj are transmitted by Opening Ob.

[0040] The transmitted seed Sj is applied to the pseudo-random generation machine 8. According to Seed's Sj operation, the pseudo-random generation machine 8 generates Data Ej. And the \*\* data Ej and Cj into which it was put are applied to the exclusive-OR function 9. The data Fj generated from the exclusive-OR function 9 are compared with Data Gj by the comparison circuit 10. If Data Ej are in agreement with Data Bj, Data Fj are in agreement with Data Gj.

[0041] It is here and is [0042].

[Equation 2]



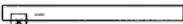
[0043] Namely, [0044]

[Equation 3]



[0045] It will be [0046] if it becomes Ej=Bj.

[Equation 4]



[0047] namely, Fj=Gj — so, the comparison operator 10 checks whether Data Fj are the same as Data Gj, or it is not the same. In such a case, Data Y are stored in Memory M. The scramble key by which the transfer of the scramble key from the smart card 1 using Challenge Handshake Authentication Protocol which was explained by drawing 1 and drawing 2 as an advantageous point to a decoder 2, on the other hand, corroborated that it was not the card with which a smart card is an authentication card and was hacked, and was transmitted to the decoder 2 on the other hand corroborates being taken out from the smart card which is not hacked truly.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] Fundamental drawing of the approach of transmitting the scramble key decrypted between the security element and the decoder by this invention is shown.

[Drawing 2] The specific embodiment of a step with the approach shown in drawing 1 is shown.

[Description of Notations]

1 Security Element

2 Decoder

3 Generation Machine of Random WORD

4 Pseudo-random Generation Machine

5 Exclusive-OR Function

6 Data Association Circuit

7 Separation Operator

8 Pseudo-random Generation Machine

9 Exclusive-OR Function

10 Comparison Circuit

---

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-196083

(43) 公開日 平成11年(1999)7月21日

(51) Int.Cl.<sup>\*</sup>

### 識別記号

F I  
H041 9/00

601B  
675A

(21) 出願番号 特願平10-293845

(22) 出願日 平成10年(1998)10月15日

(31) 优先权主张番号 9713022

(32) 価先日 1997年10月17日

(33) 優先権主張国 フランス (FR)

(71) 出願人 391000771

トムソン マルチメディア ソシエテ ア  
ノニム  
THOMSON MULTIMEDIA  
S. A.

(72)発明者 アルナルド カンビノ

(72) 発明者 ジャン-ベルナール フィッシェール  
フランス国, 94270 ル・クレムラン・ビ  
カートル, リヨン・カレ, 38

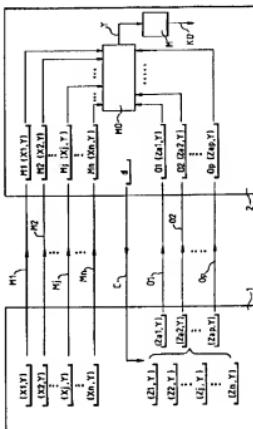
(74)代理人 助理士 伊東 宏蔵 (外1名)

(54) 【発明の名称】 スクランブルキ一転送方法

(57) 【要約】

【課題】本発明はセキュリティーエレメントからデータへスクランブルキーを転送する方法に関する

【解決手段】転送方法は、入れる段階、チャレンジ段階及びオープニング段階からなる。入れる段階では、暗号解読されたスクランブルキーを含むセキュリティーメンテはデコーダとメッセージを交換し、その結果、入れる段階の終わりにおいて、デコーダは、1対1の形で、暗号解読されたスクランブルキーの全部または部分を表すデータ及びスマートカードを認証することを可能とするデータを表すデータからなる項目を有し、チャレンジ段階では、データはデコーダからスマートカードに転送され、その結果、入れられたデータのうちのどれが開示されるかを表す。好ましくは、開示される入れられたデータの明示はランダムに行われる。オープニング段階では、スマートカードは、開示されるべきデータ、すなわち、スマートカードを認証することを可能とするデータとともに、暗号解読されたスクランブルキーの全部または部分であるデータをデコーダに転送する。



## 【特許請求の範囲】

【請求項1】セキュリティーエレメント（1）からデコーダ（2）へ暗号解読されたスクランブルキーを転送する方法において、

セキュリティーエレメント（1）から出力されたn個の最初のデータ（（X1, Y）、（X2, Y）、・・・、（Xn, Y））をデコーダ（2）の中に入れる（M1、M2、・・・、Mj、・・・、Mn）段階であって、前記nは2以上の整数であり、前記n個の最初に入れられた各データは暗号解読されたスクランブルキー（KD）の全てまたは部分（Y）及びセキュリティーエレメント（1）を認証させる最初のデータ（Xj）からなる段階と、

n個の第2のデータ（（Z1, Y）、（Z2, Y）、・・・、（Zj, Y）、・・・、（Zn, Y））からp個のデータ（（Za1, Y）、（Za2, Y）、・・・、（Zap, Y））を選択することを可能とするデータ（d）がデコーダ（2）からセキュリティーエレメント（1）へ転送されるチャレンジ（C）の段階であって、前記pはnより小さい整数であり、前記n個の第2の各データは、暗号解読されたスクランブルキーの全部または部分（Y）及びセキュリティーエレメント（1）の認証をさせる第2のデータ（Xj）からなる段階と、セキュリティーエレメント（1）からデコーダ（2）に、チャレンジ段階（C）で選択されたp個のデータの転送からなるオープニング（O1、O2、・・・、Op）の段階と、

n個の最初の入れられたデータ（（X1, Y）、（X2, Y）、・・・、（Xn, Y））から選択されたp個のデータ及びオープニング段階にて転送されたp個のデータ（O1（Za1, Y）、O2（Za2, Y）、・・・、Op（Zap, Y））から暗号解読されたスクランブルキーの全てまたは部分（Y）を抽出することを可能とする計算段階とからなることを特徴とする方法。

【請求項2】前記計算段階の後、前記入れる段階、オープニング段階及び計算段階が完全なスクランブルキー（KD）の一部分（Y）に関連する場合に、完全なスクランブルキーを再構築する段階からなる請求項1記載の方法。

【請求項3】前記入れる段階（M1、M2、・・・、Mj、・・・、Mn）は3ステップ（M1、M2、M3）からなり、オープニングステップ（O1、O2、・・・、Op）は2ステップからなる請求項1または2に記載の方法。

【請求項4】p個のデータ（（Za1, Y）、（Za2, Y）、・・・、（Zap, Y））をn個の第2のデータ（（Z1, Y）、（Z2, Y）、・・・、（Zj, Y）、・・・、（Zn, Y））から選択することはランダムに行われる請求項1ないし3のうちいずれか1項に記載の方法。

【請求項5】n個の最初に入れられたデータの各々（Cj）は、最初のデータ（Bj）及び第2のデータ（Gj）が適用される最初の排他的論理機能（5）の結果であり、前記最初のデータ（Bj）は、シード（Sj）を最初の擬似ランダム生成器（4）に適用して発生する擬似ランダムワードであり、前記第2のデータ（Gj）は、第3のデータおよび暗号解読されたスクランブルキー（Y）の全部または部分を関連させることから発生するワードであり、

前記オープニング段階はセキュリティーエレメント（1）からデコーダ（2）に、シード（Sj）及び第2のデータ（Gj）を転送することからなり、  
前記計算段階は、

シードSjを第2の擬似ランダム生成器（8）に適用することによる第4のデータ（Ej）を計算し、第5のデータ（Fj）を計算するために、第4のデータ（Ej）及び入れられたデータ（Cj）を第2の排他的論理機能（9）に適用し、

第5のデータ（Fj）をオープニングオペレーションにて転送される第2のデータ（Gj）と比較し、比較の結果、第5のデータ（Fj）がオープニングオペレーションにて転送される第2のデータ（Gj）と同一であれば、暗号解読されたスクランブルキーの全部または部分（Y）を格納することからなる請求項1ないし4のうちいずれか1項記載の方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明はスクランブルキーを転送する方法に關し、特に、条件付きアクセスシステムのセキュリティーエレメントとデコーダの間でスクランブルキーを転送する方法に関する。条件付きアクセスシステムによりサービスプロバイダは自分のサービスをそのサービスを受ける権利を獲得したユーザだけに提供することができる。このようなシステムには、例えば、有料テレビジョンシステムがある。

## 【0002】

【從來の技術】當業者に公知の如く、サービスプロバイダによって提供されたサービスは、スクランブルキーによりスクランブルをかけられた項目からなる。スクランブルをかけられた項目は、ユーザに割り当てられた権利のレベルで、スクランブルを解除せられ、ユーザに読まれる。スクランブルされた項目は以下 E（ECG）と表記される。ECGはスクランブルされていない項目を表す（ECGは“Electronically Coded Goods”的略である）。

【0003】項目をスクランブル解除するため、サービスプロバイダは、項目をスクランブルするために用いられるスクランブルキーを各ユーザに供給する。スクランブルキーを秘密に保つため、スクランブルキーはキーKを用いたアレゴリズムで暗号化された後に供給される。

種々の暗号化されたスクランブルキーは制御メッセージにおいて種々のユーザに送られる。以下、制御メッセージはECMと表記される（ECMは“Entitlement Control Message”の略である）。

【0004】権利を与えたされたユーザにだけサービスへのアクセスを与るために、サービスプロバイダは各ユーザにスマートカードとデコーダを提供する。ECMはデコーダにより受信され、デコーダはそれらをスマートカードに転送する。スマートカードはスクランブルキーの暗号化アルゴリズムのキーKを含む。スクランブルキーはスマートカードにより解読され、デコーダにリストアされ、デコーダは受信したスクランブルされた項目のスクランブル解除をすることができる。

#### 【0005】

【発明が解決しようとする課題】スマートカードとデコーダの間をモニタするハッカーは、スマートカードからデコーダへ流れる暗号解読されたスクランブルキーを傍受する位置にいる。これが欠点を表すものである。条件付きアクセスシステムはスタンダードアロンタイプのシステムであり、そのシステムではスクランブルされた項目1/E (ECG) 及びECMが、例えばデジタルビオディスクのようなスタンダードアロンの情報キャリア上に含まれているため、この欠点はさらに重大なものである。なぜならば、暗号化されていないスクランブルキーを傍受するハッカーはこれらのキーをストアでき、不正に、許可を受けていないユーザのそれらを再配布することができるからである。スタンダードアロン情報キャリア上に含まれるスクランブルされた項目はもはや保護されていないことになる。

【0006】条件付きアクセスシステムがオンラインタイプである場合、スクランブルされた項目1/E (ECG) は、空間またはケーブル上を单一の源からサービスプロバイダの種々の顧客へ同時に配布された信号から構成される項目である。解読されたスクランブルキーはリアルタイムでハック（侵害）されなければならない。ハッキングの条件はより難しくなる。しかしながら、ハッキングの危険性は十分に短いリンク上では比較的の高いままである。

【0007】本発明にはこれらの欠点がない。

#### 【0008】

【課題を解決するための手段】本発明は、セキュリティーエレメントからデコーダへ暗号解読されたスクランブルキーを転送する方法に関する。上記転送する方法は次の段階からなる。

—デコーダにおいて、セキュリティーエレメントからの最初のn個のデータ出力を（pledge）段階であり、nは2以上の整数。最初のn個の入れられた各データは、暗号解読されたスクランブルキーの全部または部分、及び、セキュリティーエレメントの認証をさせる最初のデータからなる。

【0009】—第2のn個のデータからp個のデータを選択することを可能とする1個のデータがデコーダからセキュリティーエレメントへ転送されるチャレンジの段階であり、pはnより小さい整数であり、第2のn個の各データは、暗号解読されたスクランブルキーの全部または部分、及び、セキュリティーエレメントの認証をさせる第2のデータからなる。

【0010】—チャレンジ段階の間に選択されたp個のデータをセキュリティーエレメントからデコーダへ転送することからなるオープニング段階。

—最初のn個の入れられたデータから選択されたp個のデータ、及び、オープニング段階で転送されたp個のデータから暗号解読されたスクランブルキーの全部または部分を抽出することを可能とする計算の段階。

【0011】本発明の特定の実施態様によれば、暗号解読されたスクランブルキーを転送する方法は次の通りである。

—最初のn個の入れられた各データは、最初のデータ及び第2のデータに適用される最初の排他的論理と機能の結果であり、最初のデータは、最初の擬似ランダム生成器シードを加えることから発生する擬似ランダムワードであり、第2のデータは第3のデータ、及び、暗号解読されたスクランブルキーの全部または部分と関連することから発生するワードである。

—計算の段階は次からなる。

—シードを第2の擬似ランダム生成器に適用することによる第4のデータを計算すること。

【0013】—第5のデータを計算するために、第4のデータ及び保証されたデータを、第2の排他的論理と機能に適用すること。

—第5のデータを、オープニングの動作の間に転送された第2のデータと比較すること。

—比較の結果、第5のデータがオープニングの動作の間に転送された第2のデータと同一であることがわかれれば、暗号解読されたスクランブルキーの全部または部分を格納すること。

【0014】本発明の利点は、セキュリティーエレメントとデコーダ間のデータのやりとりを保護することである。

#### 【0015】

【発明の実施の形態】本発明の他の特徴及び利点は、添付図面を参照して本発明の好ましい一実施態様を読むことにより明らかになる。添付図面において、同じ符号は同じ要素を示している。図1は、セキュリティーエレメント1とデコーダ2の間で暗号解読されたスクランブルキーを転送する方法の基本的な図を示している。セキュリティーエレメントは好ましくはスマートカードであ

る。

【0016】前述したように、スクランブルキーは、入れること (p l e d g e) の動作原理に従いスマートカード1からデコーダ2へ転送される。データを入れる動作原理は、最初の側については、予め定められたデータに関して、暗号化なしで転送することなく、第2の側に入ることからなる。次に続くステップの間、最初の側は暗号化されていないデータを第2の側に示す。第2の側は、その暗号化されていないデータが、入れられたデータと一致することを確認する可能性を有する。

【0017】本発明によれば、最初の側はスマートカード1であり、第2の側はデコーダ2であり、入れられるデータは暗号解読されたスクランブルキーの全部または部分からなる。スマートカードとデコーダの間でデータを交換するためのプロトコルは、入れる (p l e d g i n g) 段階、チャレンジ段階、オープニング段階の本質的に3つの段階からなる。

【0018】入れる段階において、暗号解読されたスクランブルキーを含むスマートカード1は、デコーダ2とメッセージを交換する。入れる段階の終わりにおいて、デコーダは、1対1の形で、暗号解読されたスクランブルキーの全部または部分を表すデータとスマートカードを認証することを可能とするデータからなる項目を有する、という方法でスマートカード1は、デコーダ2とメッセージを交換する。スマートカードを認証することを可能とするデータという用語はスマートカードがハック(侵害)されていないことを確認することを可能とするデータを意味するものと理解されるべきである。

【0019】有利な点として、保証段階の終わりにおけるデコーダに含まれる情報は、それ自身では暗号解読されたスクランブルキーの全部または部分、及びカードを認証するためのデータを得ることはできない。チャレンジ段階において、入れられたデータのうちどれが開示されるべきかを示すために、データがデコーダからスマートカードに転送される。好ましくは、開示されるべき入れられたデータを示すことは、ランダムな方法で実行される。

【0020】オープニング段階において、スマートカードはデコーダに開示されるべきデータを転送する。すなわち、暗号解読されたスクランブルキーの全部または部分、及びスマートカードを認証するためのデータを転送する。スマートカード1はデータのセット (X1、Y1)、(X2、Y2)、...、(Xn、Yn) からなる。

【0021】各データ (Xj, Yj) (j = 1, 2, ..., n) は、データYとデータXjからなる。データYは暗号解読されたスクランブルキーの全てまたは部分である。データXjはスクランブルキーとは独立で、スマートカードの認証をさせるデータである。矢印M1、M2、...、Mj、...、Mn、C、O1、O2、...、Opはスマートカード1とデコーダ2の間の種々

のやりとりを示している。

【0022】矢印M1、M2、...、Mj、...、Mnは各データ (X1, Y1)、(X2, Y2)、...、(Xn, Yn) を入れることを示している。好ましくは、データ (Xj+1, Y) のMj+1を入れることは、データ (Xj, Y) のMjを入れることに統いて行われる。本発明の好ましい実施態様によれば、入れる段階はM1、M2、M3の3ステップからなる。より一般的には、入れる段階はnステップからなり、nは2以上の整数である。

【0023】デコーダ2に入れられたデータ (Xj, Y) はMj (Xj, Y) と表される。有利な点として、前述した通り、データMj (Xj, Y) は、それ自身ではデータXjとYを識別できない。矢印Cはチャレンジ段階を示している。チャレンジ段階において、好ましくはランダムに選択されるデータdはデコーダ2からスマートカード1に転送される。データdの作用により、スマートカード1のマイクロプロセッサはスマートカードに含まれるn個のデータ (Z1, Y)、(Z2, Y)、...、(Zj, Y)、...、(Zn, Y) からp個のデータを選択し、このように選択されたp個のデータをスマートカード1からデコーダ2に転送する。

【0024】各データ (Zj, Y) (j = 1, 2, ..., n) はデータY及びデータZjからなる。本発明の最初の実施態様によれば、データZj (j = 1, 2, ..., n) はデータXjと同一であり、データ (Zj, Y) はデータ (Xj, Y) と同一である。

【0025】本発明の他の実施態様によれば、データZjはデータXjと異なる。本発明のこれから他の実施態様によれば、しかしながら、データZjはデータXjと相互関連している。データZjとデータXjの相互関連という表現は、データ (Zj, Y) 及び (Xj, Y) は、種々の回路及び/またはオペレータに適用され、データYの抽出、及び、同時にスマートカードの認証をさせる。このような実施態様の例は図2で説明される。

【0026】n個のデータ (Z1, Y)、(Z2, Y)、...、(Zj, Y)、...、(Zn, Y) から選択されるp個のデータはデータのセット (Za1, Y)、(Za2, Y)、...、(Zap, Y) からなる。p個のデータ (Za1, Y)、(Za2, Y)、...、(Zap, Y) のスマートカード1からデコーダ2への転送は、オープニングオペレーションに当たり、矢印O1、O2、...、Opはそれぞれのデータ (Za1, Y)、(Za2, Y)、...、(Zap, Y) のオープニングを表す。

【0027】それぞれのデータ (Za1, Y)、(Za2, Y)、...、(Zap, Y) のオープニングの後にデコーダ2に格納されたデータはO1 (Za1, Y)、O2 (Za2, Y)、...、Op (Zap, Y) と表される。p個の各データOk (Zak, Y) は

入れられたデータ  $M_j$  ( $X_j, Y$ ) の一つと一致する。入れられたデータ  $M_j$  ( $X_j, Y$ ) と一致するデータ  $O_k$  ( $Zak, Y$ ) という表現は、上述した本発明の最初の実施態様の場合において、データ  $Zak$  がデータ  $X_j$  と一致しているデータ  $O_k$  ( $Zak, Y$ )、または、本発明の他の実施態様の場合において、データ  $Zak$  がデータ  $X_j$  と相互関連しているデータ  $O_k$  ( $Zak, Y$ ) を意味すると理解されるべきである。

【0028】本発明によれば、デコーダ2は、データ  $M_j$  ( $X_j, Y$ ) 及び  $M_j$  ( $X_j, Y$ ) に相当するデータ  $O_k$  ( $Zak, Y$ ) からデータ  $Y$  を抽出し、スマートカード1を認証することを可能とする手段  $M$  からなる。手段  $M$  によりデータ  $Y$  がデータ  $M_j$  ( $X_j, Y$ ) 及び  $O_k$  ( $Zak, Y$ ) から抽出されると、データ  $Y$  はメモリ回路  $M$  に格納される。

【0029】本発明の好ましい実施態様によれば、入れる段階は ( $X_1, Y$ )、( $X_2, Y$ )、( $X_3, Y$ ) の3データに間連し、オープニング段階は ( $Za_1, Y$ )、( $Za_2, Y$ ) の2データに間連する。前述した通り、データ  $Y$  は暗号解読されたスクランブルキーの全部分または部分である。データ  $Y$  が暗号解読されたスクランブルキーの部分である場合、上述した入れるオペレーションはスクランブルキーを構成する種々の各部分で実行される。例を挙げるに、暗号解読されたスクランブルキーの部分である各データ  $Y$  は7または8ビットからなり、スクランブルキーは10バースで完全に再構成される。各バースは回路  $M$  によりデータ  $Y$  の抽出をさせる。暗号化されたスクランブルキー  $KD$  の完全な再構成はメモリ回路  $M$  を用いて実行される。

【0030】有利な点として、本発明によれば、データ  $Y$  のスマートカード1からデコーダ2への転送は、スマートカード1の認証と同時に行われる。それゆえ、スマートカード1はもはや認証されず、その結果、デコーダ1に転送されたデータは考慮されないので、スマートカードとデコーダの間でやりとりされるデータを傍受するハッカーは、これらのデータを変更することに意味を見出せなくなる。

【0031】図2は、図1に示された基本的な図の特定の実施態様を表す。図2においては、入れること (padding) とオープニングのオペレーションのみが表されている。スマートカード1からデコーダ2への種々の矢印は、スマートカード1とデコーダ2の間のデータの種々のやりとりを表している。

【0032】矢印  $M_j$  は、スマートカード1に含まれるデータ  $C_j$  をデコーダ2に入れるることを表している。矢印  $O_a$  及び  $O_b$  は入れるステップ  $M_j$  に相当するオープニングステップを表している。便利のため、図2に表されたスマートカード1とデコーダ2の間のデータのやりとりは、単一の入れるステップ及び単一のオープニングステップに間連している。実際、前述したように、本発

明の好ましい実施態様によれば、3データはデコーダ2に入れられ、2つのオープニングステップ ( $O_a, O_b$ ) がスマートカード1からデコーダ2に対して実行される。

【0033】図2の特定の実施態様によれば、スマートカード1はランダムワードの生成器3、擬似ランダム生成器4、排他的論理と機能5、例えばデータ連結回路のようないちごアソシエーション回路6、分離オペレータ7からなり、デコーダ2は、擬似ランダム生成器8、排他的論理と機能9、比較回路10、及び、種々のデータ  $Y$  を格納し、必要ならば種々のデータ  $Y$  から完全なキー  $KD$  を再構成する回路  $M$  からなる。

【0034】擬似データ生成器8、排他的論理と機能9及び比較回路10は回路  $M$  の例を構成する。入れられたデータ  $C_j$  は、データ  $B_j$  とデータ  $G_j$  を排他的論理と機能5に適用することにより発生する。それゆえ、

【0035】

【数1】

$$C_j = B_j \oplus G_j$$

【0036】と記述し得る。データ  $B_j$  はシード  $S_j$  が適用される生成器4から発生する擬似ランダムワードであり、シード  $S_j$  自身はランダムワードの生成器3から発生する。データ  $G_j$  は、データ  $D_j$  とデータ  $Y$  の結合から発生するワードからなる。データ  $D_j$  とデータ  $Y$  の結合は例えば連続により実行される。

【0037】本発明の好ましい実施態様によれば、データ  $Y$  は  $b$  ビットからなる暗号解読されたスクランブルキー  $KD$  の部分である。例として、 $b$  は、7または80ビットからなる暗号化されたスクランブルキーに対してそれぞれ7または8ビットに等しい。データ  $Y$  は、暗号解読されたスクランブルキー  $KD$  が適用される分離回路7から発生する。当業者には公知の如く、暗号化されたスクランブルキーはデコーダ2からスマートカード1へ転送され、スマートカード1は暗号解読されたキー  $KD$  をリストアすることを可能とする暗号解読回路(図2に記載していない)を含む。

【0038】本発明の他の実施態様によれば、データ  $Y$  は全体の暗号解読されたスクランブルキーである。本発明によれば、認証手順は、暗号化されたスクランブルキーがデコーダ2からスマートカード1へ転送される度に活性化される。擬似ランダム生成器4から発生するデータ  $B_j$  を決定することは不可能であるため、 $C_j$  の中で秘密に保たれるデータ  $G_j$  の1対1の暗号化された表現はデータ  $C_j$  である。

【0039】ワード  $C_j$  をスマートカード1からデコーダ2へ転送する、 $C_j$  の入れる段階は完了する。そして、オープニングステップが実行される。オープニングステップにおいて、2個のデータ  $S_j$  と  $G_j$  がスマートカード1からデコーダ2に転送される。データ  $S_j$  はオープニング  $O_a$  により転送され、データ  $G_j$  はオープニ

ングオブにより転送される。

【0040】転送されたシード  $S_j$  は擬似ランダム生成器 8 に適用される。シード  $S_j$  の作用により、擬似ランダム生成器 8 はデータ  $E_j$  を生成する。そして、入れられたデータ  $E_j$  と  $C_j$  は排他的論理和機能 9 に適用される。排他的論理和機能 9 から生成するデータ  $F_j$  は、比較回路 10 によりデータ  $G_j$  と比較される。データ  $E_j$  がデータ  $B_j$  と一致すれば、データ  $F_j$  はデータ  $G_j$  に一致する。

【0041】ここで

【0042】

【数2】

$$F_j = E_j \oplus C_j$$

【0043】すなわち

【0044】

【数3】

$$F_j = E_j \oplus B_j \oplus G_j$$

【0045】もし、 $E_j = B_j$  ならば、

【0046】

【数4】

$$F_j = B_j \oplus G_j$$

【0047】すなわち、 $F_j = G_j$

それゆえ、比較オペレータ 10 は、データ  $F_j$  がデータ  $G_j$  と同一か同一でないかを確認する。そのような場合は、データ  $Y$  はメモリ  $M$  に格納される。有利な点とし

て、図1及び図2で説明したような認証プロトコルを用いたスマートカード 1 からデコーダ 2 へのスクランブルキーの転送は、一方ではスマートカードが認証カードでありハッキングされたカードでないことを確認し、他方ではデコーダ 2 に転送されたスクランブルキーが本当にハッキングされていないスマートカードから出されたものであることを確認する。

【図面の簡単な説明】

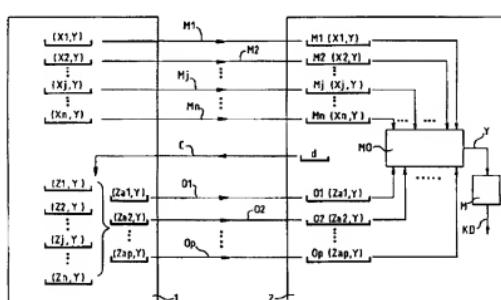
【図1】本発明により、セキュリティーエレメントとデコーダの間で暗号解読されたスクランブルキーを転送する方法の基本的な図を示している。

【図2】図1に示す方法のあるステップの特定の実施態様を示す。

【符号の説明】

- 1 セキュリティーエレメント
- 2 デコーダ
- 3 ランダムワードの生成器
- 4 擬似ランダム生成器
- 5 排他的論理和機能
- 6 データアソシエーション回路
- 7 分離オペレータ
- 8 擬似ランダム生成器
- 9 排他的論理和機能
- 10 比較回路

【図1】



【図2】

